



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

AS

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/050,675	01/15/2002	Stuart C. McClure	FNDSTN.013A	5097
28875	7590	01/20/2006		EXAMINER
Zilka-Kotab, PC P.O. BOX 721120 SAN JOSE, CA 95172-1120			SALL, EL HADJI MALICK	
			ART UNIT	PAPER NUMBER
			2157	

DATE MAILED: 01/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/050,675	MCCLURE ET AL.
	Examiner	Art Unit
	EI Hadji M. Sall	2157

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 15 January 2002.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) _____ is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-26 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ . |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>06/18/02</u> | 6) <input type="checkbox"/> Other: _____ . |

DETAILED ACTION

1. This action is responsive to the application filed on January 15, 2002. Claims 1-26 are pending. Claims 1-26 represent system and method for network vulnerability detection and reporting.

2. ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-7, 13-19 and 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini U.S. 20030101353 in view of Smith et al. "know Your Enemy: Passive fingerprinting".

As to claims 1, 13, 17 and 22, Tarquini teaches a system and a method for determining and identifying an operating system of a target computer accessible via a network, the method and system comprising the step of:

transmitting to said target computer a plurality of data packets compliant with a protocol supported by said network (page 7, [0043]);

generating a plurality of target computer fingerprints, each including at least a portion of data received via said network in response to said transmission of said plurality of data packets (page 7, [0043]);

comparing said plurality of target computer fingerprints to a first set of predetermined operating system fingerprints, each of said first set of predetermined operating system fingerprints associated with a first operating system (page 7, [0043]; page 8, [0045]).

Tarquini fails to teach explicitly generating a result indicative of whether said first operating system was running on said target .

However, Smith teaches generating a result indicative of whether said first operating system was running on said target (page 1, "The Signatures").

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tarquini in view of Smith to provide generating a result indicative of whether said first operating system was running on said target. One would be motivated to do so to allow protection of the program running in the computer against malicious hackers.

As to claims 2 and 3, Tarquini teaches the system as described in claim 1, wherein a first range of bits of said first data packet represents a first parameter value, and wherein said first range of bits of said second data packet represents a second parameter value different from said first parameter value, and wherein said second parameter value is derived by changing one bit in said first range of bits of said first data packet (page 6-7, [0038]; page 9, [0057]).

As to claim 4, Tarquini teaches the system as described in claim 2, wherein said first and second operating system fingerprints differ (page 7, [0043], Tarquini discloses comparing operating system fingerprints).

As to claims 5, 6, 16, 18 and 23, Tarquini teaches the system and method as described in claims 4, 5, 17 and 22, further comprising:

a third data packet, said third data packet compliant with said protocol, said first range of bits of said third data packet representing a third parameter value different from said first and second parameter values, said third data packet transmitted via said network to said target computer (page 7, [0043]);

a third operating system fingerprint comprising data bits stored in a computer-readable medium, said third operating system fingerprint associated with said first operating system, said third operating system fingerprint differing from said first and second operating system fingerprints (page 7, [0043], Tarquini discloses comparing operating system fingerprints); and

a third target computer fingerprint comprising data bits stored in a computer-readable medium, said third target computer fingerprint including a representation of at least a portion of data received in response to said transmission of said first data packet, said comparison instructions executable by a computer to compare said third operating system fingerprint and said third target computer fingerprint before generating said result (page 7, [0043]; page 8, [0045]).

As to claims 7, 14, 15 and 19, Tarquini teaches the system and method as described in claims 5, 13 and 17, wherein said protocol is TCP/IP and wherein said first range of bits corresponds to a packet field representing a maximum segment size (page 5, [0032]).

4. Claims 1-7, 13-19 and 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini U.S. 20030101353 in view of Smith et al. "know Your Enemy: Passive fingerprinting", further in view of Park U.S. 6,725,046.

As to claims 8-12, 20, 21 and 24-26, Tarquini teaches the system and method as described in claims 5, 10, 17 and 22.

Tarquini fails to teach explicitly said first parameter value is obtained by setting no bits, said second parameter value is obtained by setting one bit, and said third parameter value is obtained by setting two bits; wherein said first parameter value is 0,

said second parameter value is 128, and said third parameter value is 128 plus a multiple of 256; and wherein said first range of bits represents at least two bytes, and wherein a value of said second parameter is obtained by setting the last bit in a byte, and a value for said third parameter is obtained by setting the last bit in a byte.

However, Park teaches frequency list implemented using a plurality of basic frequencies and bit for use in a GSM system. Park teaches said first parameter value is obtained by setting no bits, said second parameter value is obtained by setting one bit, and said third parameter value is obtained by setting two bits; wherein said first parameter value is 0, said second parameter value is 128, and said third parameter value is 128 plus a multiple of 256; and wherein said first range of bits represents at least two bytes, and wherein a value of said second parameter is obtained by setting the last bit in a byte, and a value for said third parameter is obtained by setting the last bit in a byte (column 3, lines 13-26; column 1, lines 50-60).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tarquini in view of Part to provide said first parameter value is obtained by setting no bits, said second parameter value is obtained by setting one bit, and said third parameter value is obtained by setting two bits; wherein said first parameter value is 0, said second parameter value is 128, and said third parameter value is 128 plus a multiple of 256; and wherein said first range of bits represents at least two bytes, and wherein a value of said second parameter is obtained by setting the last bit in a byte, and a value for said third parameter is obtained by setting the last

Art Unit: 2157

bit in a byte. One would be motivated to do so to allow arrangement between the frequencies (abstract).

5.

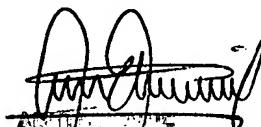
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to El Hadji M Sall whose telephone number is 571-272-4010. The examiner can normally be reached on 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on 571-272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

El Hadji Sall
Patent Examiner
Art Unit: 2157


ANJU SALL
SUPERVISORY PATENT EXAMINER
TECHNICAL CENTER 2200

